

UNITED STATES PATENT APPLICATION

FOR

Method and Apparatus for Performing a Credit Based Transaction Between a
User of a Wireless Communications Device and a Provider of a Product or
Service

INVENTORS:

Ryan J. Nobrega
Vinod V. Valloppillil

Prepared by:

Blakely, Sokoloff, Taylor & Zafman LLP
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(408) 720-8300

Attorney's Docket No. 3399P040

"Express Mail" mailing label number EL627470830US

Date of Deposit January 12, 2001

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 on the date indicated above and is addressed to the Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Julie Arango

(Typed or printed name of person mailing paper or fee)

Julie Arango
(Signature of person mailing paper or fee)

1-12-01

Method and Apparatus for Performing a Credit Based Transaction Between a
User of a Wireless Communications Device and a Provider of a Product or
Service

5 This application claims the benefit of U.S. Provisional Patent
Application no. 60/238,760, filed on October 6, 2000, and entitled, "Using the
Phone for POS Transactions", which is incorporated herein by reference.

FIELD OF THE INVENTION

10 The present invention pertains to the use of wireless communication
devices in executing credit card transactions. More particularly, the present
invention relates to using wireless communication devices in executing credit
card transactions in a manner which reduces the risk of fraudulent
transactions.

15

BACKGROUND OF THE INVENTION

Consumers have grown accustomed to using credit cards to purchase
goods and services. Although credit cards provide significant advantages
and convenience over cash transactions, various costs are associated with
20 credit card transactions. A major factor in determining the cost of a credit
card transaction is risk, and particularly, the risk of fraud. These costs may be
imposed upon merchants and consumers in the form of use charges, annual
fees, and/or higher interest rates.

There are several different ways in which a consumer can purchase
25 goods or services using a credit card, each of which has a certain amount of

fraud risk associated with it. In the traditional credit card transaction, the consumer (the credit card holder) is present at the merchant's (provider of goods or services) place of business and physically presents the card to the merchant when paying for the goods or services. The consumer physically
5 signs a paper receipt confirming the transaction. Another common type of credit card transaction type is mail order or telephone order. In this scenario, nothing is physically signed by the consumer, and the credit card is not physically present at the merchant. Consequently, this type of a credit card transaction generally involves a greater risk of fraud than an in-person
10 transaction. Another type of credit card transaction which recently has become much more common is the online (Internet) purchase. In this case as well, nothing is physically signed by the consumer, and the credit card is not physically present at the merchant. Although substantial progress has been made in the areas of data encryption and Internet security in general, this
15 method of payment is still viewed by many as involving the greatest risk of all the types of credit card transactions.

The parties potentially affected by credit card fraud include the consumer (the credit card holder), the provider of goods or services (the "merchant"), the issuer (the bank which issued the credit card), the acquirer
20 (the bank which directly interfaces with the merchant for purposes of processing a credit card transaction; often the same entity as the issuer), and the clearing network (e.g., MasterCard or Visa). These parties may be exposed to fraud in any of several ways. First, a criminal posing as a credit card account holder may make fraudulent purchases on a stolen credit card

account number. Currently, the point of origin for most of the fraud risk associated with a credit card is at the transition where the credit card is delivered from the issuer to the consumer. In addition, signatures may be forged, enabling a criminal to impersonate a legitimate credit card account holder. The transaction can be completed even if the merchant fails to check the signature or back up identification of the consumer. Furthermore, an acquirer must trust the information it receives from the merchant.

Consequently, a criminals posing as a merchant may run transactions on a stolen credit card number. Also, a criminal working for a legitimate merchant may falsify the amount of the legitimate purchase. The transaction can also be completed even if the consumer does not verify that the transaction is for the correct amount, enabling a criminal to run a fraudulent transaction amount. In addition, a consumer may repudiate a valid transaction. In the online scenario in particular, is very difficult to prove that the consumer approved the transaction.

Credit card fraud creates expense for credit card networks, their banks, and consumers. Reducing the incidence of fraud in credit card transactions will help to save money and, in turn, to reduce use charges for merchants and consumers and enable new credit card services. A new credit card payment system, therefore, should work within, and preferably improve upon, existing risk tolerance levels and other constraints associated with more conventional credit card transactions.

Furthermore, a new credit card payment system should not require significant added hardware or changes to existing merchant credit card

authorization/clearing procedures, or require significant effort or training for merchants and consumers.

SUMMARY OF THE INVENTION

The present invention includes a method and apparatus for facilitating a credit based transaction between a consumer and a provider of a product or service. The method comprises a telecommunications carrier providing
5 telecommunications services to users of wireless communications devices on a wireless communications network, including the consumer, and validating the credit card transaction between the consumer and the provider. The carrier may receive a portion of the revenue associated with credit card transactions.

10 In another aspect of the present invention, a method and apparatus for facilitating a credit based transaction between a consumer and a provider of a product or service includes storing credit account information of the consumer within a trusted domain which excludes the consumer and the provider. The credit account information is used to validate the transaction
15 between the consumer and the provider, such that the stored credit account information is not sent outside the trusted domain at any time in relation to the transaction. The method may be performed by a wireless telecommunications carrier, which may receive a portion of the revenue associated with credit card transactions.

20 Other features of the present invention will be apparent from the accompanying drawings and from the detailed description which follows.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example and not limitation in the figures of the accompanying drawings, in which like references indicate similar elements and in which:

5 Figure 1 is a block diagram illustrating the entities and the environment associated with performing a credit card transaction using a wireless device in accordance with the present invention;

Figure 2 illustrates the environment of Figure 1 in greater detail, according to one embodiment;

10 Figures 3A and 3B collectively form a flow diagram showing the overall process of performing a credit card transaction in accordance with the present invention;

Figures 4A and 4B collectively form a flow diagram showing in greater detail the validation process performed by the commerce platform, according
15 to a first embodiment;

Figures 5A and 5B collectively form a flow diagram showing in greater detail the validation process performed by the commerce platform, according to a second embodiment; and

Figures 6A through 6E show a series of screens which may be
20 displayed on a cellular telephone or the like during a credit card based transaction in accordance with the present invention.

DETAILED DESCRIPTION

A method and apparatus for performing a credit card transaction between a merchant and a consumer using a wireless communications device are described. A "merchant" is defined herein to mean a provider of goods and/or services. Note that in this description, references to "one embodiment" or "an embodiment" mean that the feature being referred to is included in at least one embodiment of the present invention. Further, separate references to "one embodiment" in this description do not necessarily refer to the same embodiment; however, neither are such embodiments mutually exclusive, unless so stated and except as will be readily apparent to those skilled in the art.

The techniques described herein provide a new modality of credit card payment that can benefit all parties involved in a credit card transaction. The described techniques help to substantially reduce the risk of fraud associated with credit card transactions and, accordingly, to reduce the costs associated with credit card transactions. In addition, the described techniques are amenable to quick and widespread acceptance in the marketplace, since they require little or no additional hardware, no significant changes to merchant authorization and clearing procedures, and little or no effort or training of merchants and consumers.

As described in greater detail below, the techniques provided herein enable a wireless telecommunications network operator ("wireless carrier") to validate the identities of credit card users who use wireless devices such as cellular telephones (and who therefore subscribe to the carrier's service), and

to ensure that the credit card users approve the transactions and receive receipts for the transactions. A wireless carrier has the capability to identify a cellular telephone (or other wireless device) and its user as part of providing its telecommunications services. Therefore, when a credit card transaction is

5 conducted in part by using the wireless device on the carrier's network, the carrier can: 1) authenticate and account holder's identity independently and redundantly to existing credit card purchase processes; 2) require that proposed credit card purchases only be executed if they are agreed to by the true credit card account holder; and 3) validate that the wireless device

10 involved in a proposed credit card transaction is located in the same geographic area as the proposed transaction.

For performing this validation process and thereby accepting a portion of the associated risk/liability, a wireless carrier may also receive a portion of the revenue associated with the credit card transactions it validates. This

15 remuneration may be provided through a business arrangement for providing the validation services. For example, the credit card issued to the consumer may be the wireless carrier's co-branded Visa, Mastercard, etc. Accordingly, a percentage of the transaction amount, which typically would have been allocated entirely to the issuer, might now go to the wireless

20 carrier. This approach is a significant departure from the risk/revenue allocation model associated with conventional credit card transactions. Of course, it will be recognized that the validation process described herein does not have to be performed by a wireless carrier and could be performed by many other types of entity or enterprise.

To accomplish the above-mentioned tasks, as described in greater detail below, an entity such as a wireless carrier maintains, owns and/or operates a commerce platform within a "trusted domain". In certain embodiments, the commerce platform stores the consumer's credit card account information and other personal information on the consumer, for purposes of validating the identity of the consumer. The merchant's point of sale (POS) terminal sends transaction information to the acquirer at the time of purchase. Based on this information, the acquirer recognizes the transaction type and responds by routing the transaction information to the commerce platform. The commerce platform may receive, for example, a personal identification number (PIN) or the like, input by the consumer at the wireless device, which the commerce platform may use in association with the stored information to verify the identity of the consumer. Note that a wireless carrier also has other ways of validating user identity for a credit card transaction besides using a PIN, such as based on its knowledge about the legitimacy of the wireless device being used and correlations between the wireless device and the issued card.

When the consumer's identity is validated, the commerce platform passes the consumer's account information (credit card number, expiration date, etc.) to the acquirer, which is also located within the trusted domain. The acquirer forwards the information to a clearing network within the trusted domain.

When the transaction clears, the acquirer notifies the commerce platform and signals the merchant's point of sale (POS) terminal to generate a

conventional paper receipt confirming the transaction. In response, the commerce platform stores a digital receipt of the transaction, which the consumer may access online using the wireless device or any other computing device having online access capability. The commerce platform may also
5 signal the wireless device to output a confirmation message to the consumer.

To be viable, a new credit card payment system must work within existing constraints associated with processing merchant credit transactions. Some of these constraints are related to attitude in the marketplace; that is, they are a consequence of the decades of entrenched merchant behavior and
10 hardware equipment in the field. Others are economic and related to the structure of the credit card economy. For example, one factor which affects any potential solution is the desirability of leveraging the credit card value chain. A large part of the reason credit cards have the presence they enjoy today is that there are potentially five players in every transaction (consumer,
15 merchant, acquirer, clearing network, and issuer), each of whom has incentive to widen the network and make transactions viable. In particular, the acquiring bank representing the merchant provides a point interface into potentially thousands of downstream merchants. Creating solutions and processes that target the acquiring bank simultaneously provides them with
20 incentive and reduces system-wide deployment hurdles.

Another factor is the desirability of integrating current merchant authorization and clearing procedures. The credit card networks have invested enormous amounts of time and effort in educating merchants about the complex process of recognizing credit card revenue. POS terminals in

particular have a large, deeply entrenched role in merchant procedures. For many retail merchants, the POS terminal is the primary (if not exclusive) accounting system for the company. A third factor is authentication and risk management. The credit industry is one of the most sophisticated consumers of risk management technologies in the world. Fine-grained actuarial tables precisely outline the costs of credit transactions across various channels (e.g., mail order vs. in-person transaction).

To gain acceptance, therefore, a system must not exceed current industry tolerances for risk and, ideally, should reduce risk. A system whose risk can be managed within current risk modeling parameters is preferred. In addition, a new credit card payment system should be easily deployable and should require little effort by, and education of, merchants and consumers.

One potential solution is the Local Proximity approach. In this approach, a cellular phone converses with the merchant's POS using short-range wireless technologies such as Blue Tooth, infrared (IR), or contactless chips. A benefit of this approach is that it would work with current merchant systems for authorization and clearing of transactions. A disadvantage, however, is that it would require introduction of new hardware to merchants that wish to participate.

Another potential solution is the "merchant electronic storefront". In this approach, the cellular phone would interact with a website belonging to a merchant (or perhaps a group of merchants) and electronically transact with this electronic storefront. A benefit of this approach is that it does not require new hardware at the merchant's location. A disadvantage is that it creates an

entirely new authorization/clearing system for merchants. Most merchants currently do not have an electronic commerce ("e-commerce") infrastructure, and those that do typically handle product fulfillment, support, etc. in a manner completely separate from their physical-world efforts.

5 Yet another potential solution is the "merchant mall". This is a permutation of the above approach, in which a third party (such as the acquiring bank) handles the construction of the merchant storefront and centrally manages it. While this solution solves the problem of storefront deployment, it does not solve the problem of integrating authorization and
10 fulfillment.

The solution provided herein (as henceforth described in greater detail) overcomes these disadvantages. The solution provided herein offers additional risk-reducing opportunities which make it an attractive solution to all risk-bearing parties involved in a credit card transaction. Sensitive user
15 information can be entirely secured within the trusted domain, in contrast with conventional credit card transactions. The techniques described herein offer, in a single solution (if so implemented), the following risk-reducing features, all of which no previous single solution provides: paper receipt; digital receipt; opportunity for ink signature (if desired); digital signature;
20 digital verification of signature; verification of consumer identity; ability to use "hidden" credit card data; and, independent initiation, verification, and approval of the transaction by the merchant and the consumer. Of course, particular embodiments of the techniques described herein need not incorporate all of these features/benefits and do not have to do so to provide

value.

The techniques of the present invention integrate easily and relatively seamlessly with current merchant processes, while requiring little or no additional hardware. Merchants are thereby enabled to retain their existing
5 processes and equipment while deriving the benefit of accepting payments through a new modality.

Refer now to Figure 1, which illustrates the entities and the environment associated with performing a credit card transaction using a wireless device, in accordance with the present invention. The consumer uses
10 a wireless communication device 1 during the credit card transaction. The wireless device 1 may be, for example, a cellular telephone, as is sometimes assumed in this description to facilitate explanation. It will be recognized, however, that the wireless device 1 could alternatively be essentially any other type of wireless communication device, such as a personal digital
15 assistant (PDA), a two-way pager, or the like. It may be assumed that the wireless device 1 includes browser software (sometimes referred to as a minibrowser or microbrowser in a hand-held wireless device). The wireless device 1 communicates with a commerce platform (CP) 2, which is located within a "trusted domain" 3, via a secure channel. Information on the
20 consumer is stored in the commerce platform 2 in a secure manner, and provided to the acquirer 4, which is also located within the trusted domain 3, when the identity of the consumer has been verified. The trusted domain 3 is a domain in which the consumer is credit card account information and other confidential/personal information of the consumer is maintained. The

trusted domain 3 excludes the merchant and the consumer. In certain
embodiments, the credit card account information and other personal
information of the consumer is never allowed to leave the trusted domain 3
during, or in connection with, the transaction. At the merchant's place of
5 business, transaction information is entered into the merchant's POS terminal
5. The merchant's POS terminal 5 interfaces directly with the acquirer 4.

During a traditional credit card transaction, the merchant's POS
terminal sends transaction information to the acquirer. During an in-person
credit card transaction, this process is typically initiated by swiping the
10 consumer's credit card through a magnetic stripe reader in the merchant's
POS terminal. Otherwise, the credit card number may be simply typed into a
numeric keypad on the POS terminal. The information transmitted to the
acquirer normally includes the consumer's credit card number, expiration
date, amount of the transaction, an identifier of the merchant, and an
15 identifier of the acquirer. The acquirer routes this information to a clearing
network (e.g., MasterCard or Visa), which determines whether the transaction
is authorized based on, among other things, the amount of credit currently
available to the consumer. If the transaction is authorized by the clearing
network, the acquirer signals this fact to merchant's POS terminal, which
20 prints a paper receipt of the transaction. The receipt is then signed by the
consumer to complete the transaction. (Not shown in Figure 1 is the issuer of
the credit card.)

In contrast, a credit card transaction in accordance with the present
invention uses independent actions of both the consumer (using a wireless

device) and the merchant (normally using a POS terminal). That is, the merchant and the consumer independently initiate, verify and approve transaction. Whereas previously the merchant would be in complete control of the transaction once the consumer had communicated the credit card information, the consumer is now involved in the initiation and approval of the transaction.

The merchant's point of sale POS terminal 5 sends transaction information to the acquirer 4 in a manner that is essentially the same as done today. However, the information sent to the acquirer 4 by the merchant's POS terminal 5 does not include the consumer's credit card information, because that information is never provided to the merchant. Based on the information it receives from the POS terminal 5, the acquirer 4 recognizes that the transaction is of a predetermined type, i.e., a transaction is to be processed using a wireless device, as opposed to a conventional credit card transaction. Upon recognizing this fact, the acquirer 4 responds by routing the received transaction information to the commerce platform 2 over a dedicated, secure channel 7 between these two parties. All communications between the acquirer and the commerce platform, as described further below, are encrypted and carried out over the dedicated, secure channel 7.

Concurrently, in one embodiment, the commerce platform 2 receives a PIN input by the consumer at the wireless device 1 and uses the PIN and stored information associated with the consumer to verify the identity of the consumer. The consumer's PIN is encrypted and non-retrievable. The PIN does not have to consist of purely numeric characters; a PIN can be a

combination of alphabetic characters and numerals, or even purely alphabetic characters. When the consumer's identity is verified, the commerce platform 2 passes the consumer's account information (e.g., credit card number and expiration date) to the acquirer 4. The acquirer 4 then forwards the

5 information to the clearing network (CN) 6 within the trusted domain 3.

When the transaction clears, the acquirer 4 notifies the commerce platform 2 of this fact and signals the merchant's POS terminal 5 to generate a conventional paper receipt confirming the transaction. Concurrently with this

action by the acquirer 4, the commerce platform 2 stores a digital receipt of
10 the transaction and signals the wireless device 1 to output a confirmation message to the consumer. The consumer may access his stored digital receipts online using the wireless device or any other computing device having online access capability, using for example a Web site interface.

The commerce platform 2 may be implemented in one or more
15 conventional computer systems, such as one or more personal computers (PCs) and/or workstations. In an embodiment in which the commerce platform 2 is formed by multiple computer systems, such computer systems may be coupled to each other on a network, such as a local area network (LAN), wide area network (WAN), or even over the Internet if a secure
20 communication link is used.

In one embodiment, the commerce platform 2 also provides the consumer with a personalized, password-protected portal to a shopping software application, which the consumer accesses using the wireless device, to initiate the credit card transaction. Note that the consumer can also

potentially access this portal using any other type of computer system with online capability.

As noted, the commerce platform 2 may be maintained and operated by the wireless carrier which provides telecommunications services to the wireless device 1 involved in the credit card transaction. Accordingly, the wireless carrier may receive a portion of the revenue associated with the transactions it validates, in exchange for accepting a portion of the risk/liability. Note, however, that many of the operations of the commerce platform 2 described herein do not have to be performed by a wireless carrier; essentially any other entity or enterprise could perform such operations. Hence, a commerce platform 2 such as described herein can potentially be maintained and operated by any entity or enterprise. It will be understood that references in this description to the commerce platform being maintained, owned and/or operated by a wireless carrier are for purposes of explanation only.

On the other hand, a wireless carrier is in a position to add significant value to a credit card payment system, by virtue of its unique relationship with users of wireless devices. Therefore, it may be desirable that the commerce platform be operated by a wireless carrier. Nonetheless, a wireless carrier may perform validation procedures such as described herein without necessarily using a commerce platform exactly as described herein.

In addition, note that aspects of the present invention can be applied without securing the credit card account information of the consumer within a trusted domain. For example, a commerce platform such as described

herein may be used to facilitate a credit card transaction using a wireless device, even though the credit card information may be provided by the consumer directly to the merchant (i.e., in the traditional manner). In that case, the commerce platform still serves to "link" the independent actions of the merchant and the actions of the consumer for purposes of carrying out the transaction.

Figure 2 illustrates the environment of Figure 1 in greater detail, according to one embodiment. It will be recognized that various other embodiments are possible. As shown, the cellular phone 1 communicates with the commerce platform 2 via a wireless communications (e.g., cellular telephone) network 21 and a gateway server 22. The gateway server 22 connects the wireless network 21 to the commerce platform 2.

In one embodiment, a primary function of the gateway server 22 is to provide a connection between the wireless network 21 and the Internet 23. This interface allows wireless devices such as cellular phones to access the World Wide Web, send and receive electronic mail (e-mail), etc. The gateway server 22 may be implemented as one or more conventional PCs and/or workstations. To provide the aforementioned functions, the gateway server 22 may include and execute software such as the UP.Link WAP Server Suite, available from Openwave Systems, Inc. of Redwood City, California.

The cellular telephone 1 may communicate with the wireless network 21 using, for example, Wireless Access Protocol (WAP). The wireless network 21 may communicate with the gateway server 22 using, for example, the Signaling System 7 (SS7) protocol. The gateway server may communicate

with other devices on the Internet using, for example Internet protocol (IP) and/or Hypertext Transfer Protocol (HTTP). The commerce platform may communicate with the gateway server using the same or similar protocols. The connection between the commerce platform and the gateway server may

5 be a direct connection or a connection via a network (e.g. a LAN).

The commerce platform 2 includes software 24 and a database 25 which contains credit card account information, PINs, and other personal information of multiple credit card holders (consumers). If the commerce platform 2 is operated by the wireless carrier (i.e., the operator of wireless

10 network), the information in the database 25 may be limited to the aforementioned information for only the cardholders who subscribe to the wireless carrier's services. The software 24 within the commerce platform 2 enables it to perform the identity verification operations described above. In one embodiment, the software 24 within the commerce platform 2 includes a

15 portal built on top of the MyPhone system, available from Openwave Systems, Inc. The MyPhone system provides a mobile portal platform and a suite of value-added communication applications and personal information management (PIM) applications that enable development of next generation universal access Internet portals. The portal provides the consumer with

20 access to an e-commerce (shopping) software application, which may also reside and/or execute in the commerce platform 2.

The merchant's POS terminal 5 communicates with the acquirer 4 through a standard dial-up connection through, for example, the public switched telephone network (PSTN) 26. The commerce platform 2

communicates with the acquirer 4 over a secure, dedicated channel 7. The secure, dedicated channel 7 may be a virtual private network (VPN) connection on and otherwise nonsecure public network, such as the Internet 23.

5 The overall process of performing a credit card transaction according to the present invention is now further described with reference to Figures 3A and 3B, which illustrate one embodiment of such a process. At processing block 301, the consumer initially presents merchandise for payment at a checkout location at the merchant's place of business. At block 302, the
10 merchant inputs information into a conventional transaction recording device, such as a bar code scanner, cash register, or notepad. When the merchant asks the consumer for the method of payment, the consumer informs the merchant the merchandise will be paid for using the consumer's phone. Note that the consumer does not present a credit card or communicate his credit
15 card number to the merchant at this time or at any other time during the transaction. Next, at block 303, the merchant's POS terminal sends transaction information to the acquirer. The contents of this transmitted information can vary from embodiment to embodiment, as discussed below. However, this information normally includes some type of indicator which allows the
20 acquirer to identify this transaction as one which will be performed using the consumer's phone. Next, at block 304, the acquirer identifies the transaction type based on the information received from the merchant, and responds by passing the transaction amount, a unique identifier of the merchant (MerchantID), a unique identifier of the merchant's POS terminal

(TerminalID), and the merchant's name (Merchant Name) to the commerce platform over the secure, dedicated channel. The Merchant Name may be stored at the acquirer such that it can be looked up if the MerchantID is provided.

5 Next, at block 305, the commerce platform stores the transaction information and validates the transaction by verifying the consumer's identity, in a manner described below. (If the commerce platform is unable to validate the transaction, it sends an appropriate denial-of-transaction message to the consumer's phone, where the message is displayed to the user.)

10 Assuming the transaction is validated, at block 306, the commerce platform generates and sends to the acquirer a transaction request on behalf of the merchant and the consumer. The transaction request includes the stored transaction information and the consumer's credit card account number and expiration date. The transaction request also includes a unique
15 identifier of the acquirer, which is used for routing purposes to specify which acquiring organization should receive the transaction request. Because all relevant transactional data is now known to the commerce platform, the transaction appears from the acquirer's point of view essentially like any standard transaction initiated at a POS using a traditional credit card.

20 At block 307, the acquirer receives the transaction request and, as with any other transaction request, initiates the approval process through the clearing network. While the transaction is being processed, the commerce platform may send a message to the cellular phone to cause the phone to display a message to the consumer indicating that the transaction is pending,

such as the message shown in Figure 6D.

Assuming the transaction is approved by the clearing network, then at block 308, the acquirer passes information indicating the transaction has been cleared, including an approval authorization number and amount, to the
5 commerce platform. Because the acquirer has previously identified this transaction as a phone based transaction, and the transaction was initiated over the secure channel by the commerce platform, the acquirer recognizes that the verified transaction information must be forwarded to the commerce platform. When the commerce platform receives this information, it stores a
10 digital receipt of the transaction in association with the identity of this consumer / portal user at block 309. As noted, this digital receipt can then be accessed by the consumer using the browser on the cellular phone or any other computer system. At block 310, the commerce platform sends, via the wireless network, a message confirming completion of the transaction to the
15 consumer's phone, where the confirmation message is displayed to the consumer. An example of the confirmation message is shown in Figure 6E. In addition, as in a conventional credit card transaction, at block 311 the acquirer sends a signal to the merchant's POS terminal, including the approval authorization number and amount, indicating that the transaction
20 has cleared and instructing it to generate a paper receipt. At block 312, the merchant's POS terminal prints the paper receipt, which is delivered to the consumer.

The process is complete at this point. Note that in contrast with a conventional in-person credit card transaction, the consumer's physical (pen

and ink) signature is not required. Note, however, that the opportunity for the merchant to obtain the consumer's physical signature is still present, since a paper receipt is printed. Therefore, the merchant can obtain a physical signature if desired. However, with this technique, a physical signature
5 would likely provide little or no added value.

Figures 4A and 4B collectively show in greater detail the validation process (block 305) performed by the commerce platform, according to one embodiment. In this embodiment, the merchant enters a pre-defined transaction type identifier (e.g., "type=phone") into the POS terminal to
10 signify that: 1) the consumer's identity has not yet been identified/verified; and 2) a wireless application will be used to provide and/or verify identity and transaction data. The transaction type identifier may be input by the merchant in place of a credit card number. The transaction may look something like the following when viewing the display of the merchant's POS
15 terminals:

POS: "Slide Card or Enter Card #"
MERCHANT input: 2211 (code specifying no card available; phone transaction)
POS: "Enter Amount"
20 Merchant input: \$102.10

Along with the transaction information manually entered by the merchant, the following additional data is sent automatically by the POS terminal: MerchantID, TerminalID, TransactionType, and Amount.

25 As noted above, upon receiving information from the POS terminal and recognizing the transaction type, the acquirer forwards the received information to the commerce platform. Referring now to Figure 4A, the

commerce platform receives the transaction information from the acquirer at block 401 and stores it along with a unique identifier of the acquirer

(AcquirerID) and the date and time at which the information is received. The commerce platform then generates a unique session ID at block 402. The

5 session ID will be used by the consumer to identify the transaction that is desired. At block 403 the commerce platform sends the session ID to the acquirer. The acquirer then passes the session ID to the merchant's POS terminal at block 404. The session ID is then communicated to the consumer at block 405. This can be done by the POS terminal, an ancillary terminal-type
10 device with a larger/more presentable display, and/or verbally by the merchant. The session ID can alternatively be communicated directly from the merchant's equipment to the wireless device, using a technology such as Blue Tooth, IR, or contactless chips. The method of delivery may depend upon the complexity of the session ID. For instance, if the session ID is a
15 simple integer (such as "0321") it may be effectively communicated orally by the merchant. However, if the session ID is more complex (such as "0321-45678"), it may be more effectively conveyed to the consumer via a digital display.

The generation of the session ID and its presentation to the consumer
20 offers the opportunity to "close the loop" and identify the consumer. This is accomplished by providing a phone application to the user, via the commerce platform, which allows the user to associate himself with the newly acquired session ID. Hence, the consumer uses the phone's browser at block 406 to navigate to a known shopping application, via the above-mentioned portal.

To access the portal, the user will be prompted to enter any username and password. When prompted, the consumer inputs his PIN (as shown in Figure 6B) and the session ID into the cellular phone at block 407, which information is transmitted to the commerce platform at block 408.

5 For example, the user might enter a pre-defined "buy from merchant" section of the portal and be prompted to enter the PIN and session ID. The processing flow through this application may be as follows: 1) start the phone's minibrowser; 2) log in to the portal with username and password (this establishes the user/consumer's identity); 3) navigate through various
10 menu selections to shopping application; 4) enter PIN; and 5) enter session ID. This information is then passed to the commerce platform over a secure channel.

 The commerce platform receives this information at block 409, and uses it to verify the consumer's identity at block 410. The commerce platform
15 verifies the consumer's identify by both authenticating the consumer against the portal itself and then by verifying the consumer's PIN. (If the consumer's identity cannot be verified, the commerce platform sends an appropriate denial-of-transaction message to the cellular phone, where it is displayed to the consumer.) At block 411, the commerce platform uses the session ID
20 received from the cellular phone to look up the transaction information which it previously received from the acquirer and stored. The session ID is the key to "closing the loop", since it is the only piece of information that is known to all parties involved. The previously stored time/date of the session ID is also evaluated at this time to ensure the session ID is still valid. (If the commerce

platform is unable to locate the storage transaction information, it sends an appropriate denial of transaction message to the cellular phone, where the message is displayed to the consumer.) At block 412, the commerce platform sends to the cellular phone information indicating the details of the transaction (e.g. Merchant Name, Amount, etc.) and a prompt for the consumer either to accept or to decline the proposed transaction, where this information and prompt is displayed to the consumer. An example of what might be displayed to the consumer on the cellular phone is shown in Figure 6A.

Assuming the consumer accepts the transaction and provides an input to the cellular phone indicating such acceptance, and acceptance signal is transmitted from the cellular phone to the commerce platform. At this point, the verification process is complete, and the process flow returns to the main process, where processing continues from block 307 in Figure 3A.

In the commerce platform, stored along with the credit card number in the consumer's profile can also be an encrypted token that further identifies the consumer, the credit card number and type being used, and/or the authenticity of the request to the acquirer. This information may not be necessary given the nature of the transaction however (it is used in a physical credit card to prove that the card was present at the time of transaction. Since the physical "credit card" is now replaced by an interactive device in the form of a wireless device, the consumer can independently verify the transaction using his PIN and by interacting with the confirmation dialogue).

Figures 5A and 5B collectively show in greater detail the validation

process (block 305) performed by the commerce platform, according to a second embodiment. Note that strictly speaking, blocks 301A through 304A can be considered separate from the validation process but are nonetheless included in Figure 5A for clarity. In this embodiment, the consumer

5 communicates a unique ID to the merchant at block 301A, to initiate the transaction. The unique ID is used to identify the transaction as a phone based transaction and may be, for example, the consumer's cellular telephone number. The unique ID can alternatively be communicated directly from the wireless device to the merchant's equipment, using a technology such as Blue
10 Tooth, IR, or contactless chips, or by scanning a bar code on the wireless device. At block 302A, the merchant inputs the consumer's unique ID into the POS terminal, substituting the unique ID for a credit card number. At block 303A, the merchant's POS terminal sends the transaction information with the unique ID to the acquirer. At block 304A, the acquirer then identifies the
15 transaction type as being a phone based transaction based on the unique ID, and passes the unique ID, the Amount, MerchantID, TerminalID, and Merchant Name to the commerce platform. If the commerce platform is operated by a wireless carrier, the acquirer also maps the unique ID to the appropriate wireless carrier (i.e., the appropriate commerce platform) for the
20 consumer's cellular phone in block 304A.

The validation process (block 305) then begins with block 501 in Figure 5A. It is assumed for this embodiment that the commerce platform is owned and/or operated by the wireless carrier associated with the consumer's cellular phone. At block 501, the commerce platform identifies the user

account associated with the unique ID. At block 502, the commerce platform verifies that the phone involved in the transaction is in the same geographic area as the merchant. This can be done using standard location technology in cellular telephones and cellular telephone networks. Note that the cellular

5 phone automatically transmits its unique identifier (handset ID) to the wireless carrier when it is turned on. If the verification of block 502 fails, an appropriate message is sent to the cellular phone, for display to the user. At block 503, the commerce platform sends the transaction details and a prompt to accept or decline the transaction to the phone associated with the identified

10 user account, where the message is displayed to the user. Assuming the consumer accepts the transaction (using appropriate input to the cellular phone) at block 504, the consumer will next be prompted to enter his PIN at block 505. After the consumer inputs his PIN into the phone at block 506, the phone transmits the PIN to the commerce platform at block 507. At block 508,

15 the commerce platform uses the PIN to verify the user's identity against previously established accounts. (If verification fails, an appropriate message is sent to the phone, where it is displayed to the consumer.) The commerce platform then causes the consumer's phone to prompt the consumer to indicate the method of payment at block 509. An example of such a prompt is

20 shown in Figure 6C. The consumer selects the method of payment at block 510, and the method of payment selection is transmitted to the commerce platform at block 511. At this point, the verification process is complete, and the process flow returns to the main process, where processing continues from block 307 in Figure 3A. Note that, as in the previously described

embodiment, there may be a time to live (TTL) associated with each transaction, which the commerce platform evaluates.

Of course, there are many possible permutations of the above-described embodiments, which may fall within the scope of the present

5 invention. As noted above, it is not essential that the credit card information of the consumer be isolated within a trusted domain. The process of verifying the identity of the consumer may be done in a traditional manner, such that the commerce platform plays a more limited role. As one example, identification of the consumer may be accomplished using a simple
10 identification card issued to the consumer by an authorized entity (e.g., the government). In that case, the commerce platform still serves to link the independent actions of the consumer and the merchant to a particular proposed transaction.

As another example, the consumer may be issued a credit card that
15 references an existing portal account maintained by the commerce platform for cellular phone-based authorization. A transaction initiated by the merchant would then remain at the acquirer for a predefined TTL and await possible confirmation by the consumer by cellular phone. In this scenario, a discount could be applied to the transaction if the consumer confirms by
20 telephone before the TTL expires, as a consequence of the reduced risk. Otherwise, the transaction could be completed as a traditional credit card transaction.

Thus, a method and apparatus for performing a credit card transaction between a merchant and a consumer using a wireless communications device

have been described. Although the present invention has been described with reference to specific exemplary embodiments, it will be evident that various modifications and changes may be made to these embodiments without departing from the broader spirit and scope of the invention as set forth in the
5 claims. Accordingly, the specification and drawings are to be regarded in an illustrative sense rather than a restrictive sense.

11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207 208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223 224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239 240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255 256 257 258 259 260 261 262 263 264 265 266 267 268 269 270 271 272 273 274 275 276 277 278 279 280 281 282 283 284 285 286 287 288 289 290 291 292 293 294 295 296 297 298 299 300 301 302 303 304 305 306 307 308 309 310 311 312 313 314 315 316 317 318 319 320 321 322 323 324 325 326 327 328 329 330 331 332 333 334 335 336 337 338 339 340 341 342 343 344 345 346 347 348 349 350 351 352 353 354 355 356 357 358 359 360 361 362 363 364 365 366 367 368 369 370 371 372 373 374 375 376 377 378 379 380 381 382 383 384 385 386 387 388 389 390 391 392 393 394 395 396 397 398 399 400 401 402 403 404 405 406 407 408 409 410 411 412 413 414 415 416 417 418 419 420 421 422 423 424 425 426 427 428 429 430 431 432 433 434 435 436 437 438 439 440 441 442 443 444 445 446 447 448 449 450 451 452 453 454 455 456 457 458 459 460 461 462 463 464 465 466 467 468 469 470 471 472 473 474 475 476 477 478 479 480 481 482 483 484 485 486 487 488 489 490 491 492 493 494 495 496 497 498 499 500 501 502 503 504 505 506 507 508 509 510 511 512 513 514 515 516 517 518 519 520 521 522 523 524 525 526 527 528 529 530 531 532 533 534 535 536 537 538 539 540 541 542 543 544 545 546 547 548 549 550 551 552 553 554 555 556 557 558 559 560 561 562 563 564 565 566 567 568 569 570 571 572 573 574 575 576 577 578 579 580 581 582 583 584 585 586 587 588 589 590 591 592 593 594 595 596 597 598 599 600 601 602 603 604 605 606 607 608 609 610 611 612 613 614 615 616 617 618 619 620 621 622 623 624 625 626 627 628 629 630 631 632 633 634 635 636 637 638 639 640 641 642 643 644 645 646 647 648 649 650 651 652 653 654 655 656 657 658 659 660 661 662 663 664 665 666 667 668 669 670 671 672 673 674 675 676 677 678 679 680 681 682 683 684 685 686 687 688 689 690 691 692 693 694 695 696 697 698 699 700 701 702 703 704 705 706 707 708 709 710 711 712 713 714 715 716 717 718 719 720 721 722 723 724 725 726 727 728 729 730 731 732 733 734 735 736 737 738 739 740 741 742 743 744 745 746 747 748 749 750 751 752 753 754 755 756 757 758 759 760 761 762 763 764 765 766 767 768 769 770 771 772 773 774 775 776 777 778 779 780 781 782 783 784 785 786 787 788 789 790 791 792 793 794 795 796 797 798 799 800 801 802 803 804 805 806 807 808 809 810 811 812 813 814 815 816 817 818 819 820 821 822 823 824 825 826 827 828 829 830 831 832 833 834 835 836 837 838 839 840 841 842 843 844 845 846 847 848 849 850 851 852 853 854 855 856 857 858 859 860 861 862 863 864 865 866 867 868 869 870 871 872 873 874 875 876 877 878 879 880 881 882 883 884 885 886 887 888 889 890 891 892 893 894 895 896 897 898 899 900 901 902 903 904 905 906 907 908 909 910 911 912 913 914 915 916 917 918 919 920 921 922 923 924 925 926 927 928 929 930 931 932 933 934 935 936 937 938 939 940 941 942 943 944 945 946 947 948 949 950 951 952 953 954 955 956 957 958 959 960 961 962 963 964 965 966 967 968 969 970 971 972 973 974 975 976 977 978 979 980 981 982 983 984 985 986 987 988 989 990 991 992 993 994 995 996 997 998 999 1000 1001 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018 1019 1020 1021 1022 1023 1024 1025 1026 1027 1028 1029 1030 1031 1032 1033 1034 1035 1036 1037 1038 1039 1040 1041 1042 1043 1044 1045 1046 1047 1048 1049 1050 1051 1052 1053 1054 1055 1056 1057 1058 1059 1060 1061 1062 1063 1064 1065 1066 1067 1068 1069 1070 1071 1072 1073 1074 1075 1076 1077 1078 1079 1080 1081 1082 1083 1084 1085 1086 1087 1088 1089 1090 1091 1092 1093 1094 1095 1096 1097 1098 1099 1100 1101 1102 1103 1104 1105 1106 1107 1108 1109 1110 1111 1112 1113 1114 1115 1116 1117 1118 1119 1120 1121 1122 1123 1124 1125 1126 1127 1128 1129 1130 1131 1132 1133 1134 1135 1136 1137 1138 1139 1140 1141 1142 1143 1144 1145 1146 1147 1148 1149 1150 1151 1152 1153 1154 1155 1156 1157 1158 1159 1160 1161 1162 1163 1164 1165 1166 1167 1168 1169 1170 1171 1172 1173 1174 1175 1176 1177 1178 1179 1180 1181 1182 1183 1184 1185 1186 1187 1188 1189 1190 1191 1192 1193 1194 1195 1196 1197 1198 1199 1200 1201 1202 1203 1204 1205 1206 1207 1208 1209 1210 1211 1212 1213 1214 1215 1216 1217 1218 1219 1220 1221 1222 1223 1224 1225 1226 1227 1228 1229 1230 1231 1232 1233 1234 1235 1236 1237 1238 1239 1240 1241 1242 1243 1244 1245 1246 1247 1248 1249 1250 1251 1252 1253 1254 1255 1256 1257 1258 1259 1260 1261 1262 1263 1264 1265 1266 1267 1268 1269 1270 1271 1272 1273 1274 1275 1276 1277 1278 1279 1280 1281 1282 1283 1284 1285 1286 1287 1288 1289 1290 1291 1292 1293 1294 1295 1296 1297 1298 1299 1300 1301 1302 1303 1304 1305 1306 1307 1308 1309 1310 1311 1312 1313 1314 1315 1316 1317 1318 1319 1320 1321 1322 1323 1324 1325 1326 1327 1328 1329 1330 1331 1332 1333 1334 1335 1336 1337 1338 1339 1340 1341 1342 1343 1344 1345 1346 1347 1348 1349 1350 1351 1352 1353 1354 1355 1356 1357 1358 1359 1360 1361 1362 1363 1364 1365 1366 1367 1368 1369 1370 1371 1372 1373 1374 1375 1376 1377 1378 1379 1380 1381 1382 1383 1384 1385 1386 1387 1388 1389 1390 1391 1392 1393 1394 1395 1396 1397 1398 1399 1400 1401 1402 1403 1404 1405 1406 1407 1408 1409 1410 1411 1412 1413 1414 1415 1416 1417 1418 1419 1420 1421 1422 1423 1424 1425 1426 1427 1428 1429 1430 1431 1432 1433 1434 1435 1436 1437 1438 1439 1440 1441 1442 1443 1444 1445 1446 1447 1448 1449 1450 1451 1452 1453 1454 1455 1456 1457 1458 1459 1460 1461 1462 1463 1464 1465 1466 1467 1468 1469 1470 1471 1472 1473 1474 1475 1476 1477 1478 1479 1480 1481 1482 1483 1484 1485 1486 1487 1488 1489 1490 1491 1492 1493 1494 1495 1496 1497 1498 1499 1500 1501 1502 1503 1504 1505 1506 1507 1508 1509 1510 1511 1512 1513 1514 1515 1516 1517 1518 1519 1520 1521 1522 1523 1524 1525 1526 1527 1528 1529 1530 1531 1532 1533 1534 1535 1536 1537 1538 1539 1540 1541 1542 1543 1544 1545 1546 1547 1548 1549 1550 1551 1552 1553 1554 1555 1556 1557 1558 1559 1560 1561 1562 1563 1564 1565 1566 1567 1568 1569 1570 1571 1572 1573 1574 1575 1576 1577 1578 1579 1580 1581 1582 1583 1584 1585 1586 1587 1588 1589 1590 1591 1592 1593 1594 1595 1596 1597 1598 1599 1600 1601 1602 1603 1604 1605 1606 1607 1608 1609 1610 1611 1612 1613 1614 1615 1616 1617 1618 1619 1620 1621 1622 1623 1624 1625 1626 1627 1628 1629 1630 1631 1632 1633 1634 1635 1636 1637 1638 1639 1640 1641 1642 1643 1644 1645 1646 1647 1648 1649 1650 1651 1652 1653 1654 1655 1656 1657 1658 1659 1660 1661 1662 1663 1664 1665 1666 1667 1668 1669 1670 1671 1672 1673 1674 1675 1676 1677 1678 1679 1680 1681 1682 1683 1684 1685 1686 1687 1688 1689 1690 1691 1692 1693 1694 1695 1696 1697 1698 1699 1700 1701 1702 1703 1704 1705 1706 1707 1708 1709 1710 1711 1712 1713 1714 1715 1716 1717 1718 1719 1720 1721 1722 1723 1724 1725 1726 1727 1728 1729 1730 1731 1732 1733 1734 1735 1736 1737 1738 1739 1740 1741 1742 1743 1744 1745 1746 1747 1748 1749 1750 1751 1752 1753 1754 1755 1756 1757 1758 1759 1760 1761 1762 1763 1764 1765 1766 1767 1768 1769 1770 1771 1772 1773 1774 1775 1776 1777 1778 1779 1780 1781 1782 1783 1784 1785 1786 1787 1788 1789 1790 1791 1792 1793 1794 1795 1796 1797 1798 1799 1800 1801 1802 1803 1804 1805 1806 1807 1808 1809 1810 1811 1812 1813 1814 1815 1816 1817 1818 1819 1820 1821 1822 1823 1824 1825 1826 1827 1828 1829 1830 1831 1832 1833 1834 1835 1836 1837 1838 1839 1840 1841 1842 1843 1844 1845 1846 1847 1848 1849 1850 1851 1852 1853 1854 1855 1856 1857 1858 1859 1860 1861 1862 1863 1864 1865 1866 1867 1868 1869 1870 1871 1872 1873 1874 1875 1876 1877 1878 1879 1880 1881 1882 1883 1884 1885 1886 1887 1888 1889 1890 1891 1892 1893 1894 1895 1896 1897 1898 1899 1900 1901 1902 1903 1904 1905 1906 1907 1908 1909 1910 1911 1912 1913 1914 1915 1916 1917 1918 1919 1920 1921 1922 1923 1924 1925 1926 1927 1928 1929 1930 1931 1932 1933 1934 1935 1936 1937 1938 1939 1940 1941 1942 1943 1944 1945 1946 1947 1948 1949 1950 1951 1952 1953 1954 1955 1956 1957 1958 1959 1960 1961 1962 1963 1964 1965 1966 1967 1968 1969 1970 1971 1972 1973 1974 1975 1976 1977 1978 1979 1980 1981 1982 1983 1984 1985 1986 1987 1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025 2026 2027 2028 2029 2030 2031 2032 2033 2034 2035 2036 2037 2038 2039 2040 2041 2042 2043 2044 2045 2046 2047 2048 2049 2050 2051 2052 2053 2054 2055 2056 2057 2058 2059 2060 2061 2062 2063 2064 2065 2066 2067 2068 2069 2070 2071 2072 2073 2074 2075 2076 2077 2078 2079 2080 2081 2082 2083 2084 2085 2086 2087 2088 2089 2090 2091 2092 2093 2094 2095 2096 2097 2098 2099 2100 2101 2102 2103 2104 2105 2106 2107 2108 2109 2110 2111 2112 2113 2114 2115 2116 2117 2118 2119 2120 2121 2122 2123 2124 2125 2126 2127 2128 2129 2130 2131 2132 2133 2134 2135 2136 2137 2138 2139 2140 2141 2142 2143 2144 2145 2146 2147 2148 2149 2150 2151 2152 2153 2154 2155 2156 2157 2158 2159 2160 2161 2162 2163 2164 2165 2166 2167 2168 2169 2170 2171 2172 2173 2174 2175 2176 2177 2178 2179 2180 2181 2182 2183 2184 2185 2186 2187 2188 2189 2190 2191 2192 2193 2194 2195 2196 2197 2198 2199 2200 2201 2202 2203 2204 2205 2206 2207 2208 2209 2210 2211 2212 2213 2214 2215 2216 2217 2218 2219 2220 2221 2222 2223 2224 2225 2226 2227 2228 2229 2230 2231 2232 2233 2234 2235 2236 2237 2238 2239 2240 2241 2242 2243 2244 2245 2246 2247 2248 2249 2250 2251 2252 2253 2254 2255 2256 2257 2258 2259 2260 2261 2262 2263 2264 2265 2266 2267 2268 2269 2270 2271 2272 2273 2274 2275 2276 2277 2278 2279 2280 2281 2282 2283 2284 2285 2286 2287 2288 2289 2290 2291 2292 2293 2294 2295 2296 2297 2298 2299 2300 2301 2302 2303 2304 2305 2306 2307 2308 2309 2310 2311 2312 2313 2314 2315 2316 2317 2318 2319 2320 2321 2322 2323 2324 2325 2326 2327 2328 2329 2330 2331 2332 2333 2334 2335 2336 2337 2338 2339 2340 2341 2342 2343 2344 2345 2346 2347 2348 2349 2350 2351 2352 2353 2354 2355 2356 2357 2358 2359 2360 2361 2362 2363 2364 2365 2366 2367 2368 2369 2370 2371 2372 2373 2374 2375 2376 2377 2378 2379 2380 2381 2382 2383 2384 2385 2386 2387 2388 2389 2390 2391 2392 2393 2394 2395 2396 2397 2398 2399 2400 2401 2402 2403 2404 2405 2406 2407 2408 2409 2410 2411 2412 2413 2414 2415 2416 2417 2418 2419 2420 2421 2422 2423 2424 2425 2426 2427 2428 2429 2430 2431 2432 2433 2434 2435 2436 2437 2438 2439 2440 2441 2442 2443 2444 2445 2446 2447 2448 2449 2450 2451 2452 2453 2454 2455 2456 2457 2458 2459 2460 2461 2462 2463 2464 2465 2466 2467 2468 2469 2470 2471 2472 2473 2474 2475 2476 2477 2478 2479 2480 2481 2482 2483 2484 2485 2486 2487 2488 2489 2490 2491 2492 2493 2494 2495 2496 2497 2498 2499 2500 2501 2502 2503 2504 2505 2506 2507 2508 2509 2510 2511 2512 2513 2514 2515 2516 2517 2518 2519 2520 2521 2522 2523 2524 2525 2526 2527 2528 2529 2530 2531 2532 2533 2534 2535 2536 2537 2538 2539 2540 2541 2542 2543 2544 2545 2546 2547 2548 2549 2550 2551 2552 2553 2554 2555 2556 2557 2558 2559 2560 2561 2562 2563 2564 2565 2566 2567 2568 2569 2570 2571 2572 2573 2574 2575 2576 2577 2578 2579 2580 2581 2582 2583 2584 2585 2586 2587 2588 2589 2590 2591 2592 2593 2594 2595 2596 2597 2598 2599 2600 2601 2602 2603 2604 2605 2606 2607 2608 2609 2610 2611 2612 2613 2614 2615 2616 2617 2618 2619 2620 2621 2622 2623 2624 2625 2626 2627 2628 2629 2630 2631 2632 2633 2634 2635 2636 2637 2638 2639 2640 2641 2642 2643 2644 2645 2646 2647 2648 2649 2650 2651 2652 2653 2654 2655 2656 2657 2658 2659 2660 2661 2662 2663 2664 2665 2666 2667 2668 2669 2670 2671 2672 2673 2674 2675 2676